REMARKS

Claims 1-14 remain in the application, and new independent claim 15 has been added hereby.

The claims have been carefully reviewed with particular attention to the points raised in the Office Action. It is submitted that no new matter has been added and no new issues have been raised by the present response.

Reconsideration is respectfully requested of the rejection of claim 1 under 35 U.S.C. § 103(a), as allegedly being unpatentable over U.S. Patent No. 5,535,276 to Ganesan in view of Schneier, ''Applied Cryptography,'' p. 173 (1996) (hereinafter ''Schneier'').

Applicants have carefully considered the comments of the Office Action and the cited reference, and respectfully submit that amended independent claim 1 is patentably distinct over the cited references for at least the following reasons.

The present invention relates to a method and apparatus for mutual authentication of components in a network using a challenge-response method. At least one data pair including a first random number and a first response are requested from an authentication center. The first random number is passed to a terminal which uses an internally stored key and the first random number to calculate the first response.

The calculated first response is sent to the network, and a second response calculated in the authentication center is sent in response to a second random number. The first response sent from the terminal to the network is used as the second random number. The network has previously requested

the second response from the authorization center together with the first random number and the first response as a triplet data set.

Ganesan, as understood by Applicants, relates to an improved system and method for securing communications using split private key asymmetric cryptography. In a system utilizing a Kerberos protocol, system users each have an associated asymmetric crypto-key, and the security of communications over the system is enhanced by a first user generating a temporary asymmetric crypto-key having a first temporary key portion and an associated second temporary key portion. The second temporary key portion is encrypted by the first user with the first private key portion of the first user crypto-key to form a first encrypted message. Another user, preferably an authentication server, applies the second private key portion and the public key portion of the first user crypto-key to the first encrypted message to decrypt the second temporary key portion, thereby authenticating the first user to the security server. The authentication server then encrypts the first encrypted message with the second private key portion of the first user crypto-key to form a second encrypted message. The first user next applies the public key portion of the first user crypto-key to decrypt the second encrypted message and obtain the second temporary key portion, thereby authenticating the security server to the first user.

The Office Action notes that Ganesan does not disclose keys using random numbers (see Office Action, p. 3, ln. 16). Schneier is cited as allegedly disclosing the missing feature.

The cited portion of Schneier, as understood by Applicants, relates to random keys, and specifically to keys made of random-bit strings generated by some automatic process.

It is respectfully submitted that Ganesan relates to a method for securing communications using split private key asymmetric cryptography, and does not disclose or suggest a method for mutual authentication of components in a communication network using a challenge-response method.

As understood by Applicants, in the system of Ganesan a plurality of messages are exchanged between a client and several entities (see Ganesan, col. 15, lns. 27-31; Fig. 2). For example, messages 1' through 6' in the system of Ganesan are exchanged between a client and an authentication server (AS)(Fig. 2, element 120), a ticket granting server (TGS)(Fig. 2, element 140), and a server (Fig. 2, element 150).

In contrast, in the challenge-response method of the present invention, messages are exchanged between only two entities, the terminal and the network.

The Office Action cites column 15, lines 33-60 of Ganesan as allegedly disclosing a client request that requests authentication services and a new data pair from an authentication server (see Office Action, p. 2, lns. 14-21). The Office action apparently states that message 1 of Ganesan discloses challenge 1 of the method of the present application (see id.).

As understood by Applicants, message 1 of Ganesan is sent from the client (see Ganesan, Fig. 2, element 110) to the

authentication server (see id., element 120). The authentication server responds to the client with message 2.

Additionally, the Office Action apparently states that message 4 of Ganesan discloses challenge 1 and response 1 of the method of the present application (see Office Action, p. 2, ln. 22 to p. 3, ln. 3).

It is respectfully submitted that message 1 of Ganesan is exchanged between the client and the authentication server as described above, while message 4 of Ganesan is exchanged between the ticket granting server (see Ganesan, Fig. 2, element 140) and the client (see id., element 110).

The Office Action also apparently states that messages 5' and 6' of Ganesan disclose challenge 2 and response 2 of the method of the present application (see Office Action, p. 3, lns. 4-15).

As understood by Applicants, however, messages 5' and 6' of Ganesan are exchanged between the client and the service server (see Ganesan, Fig. 2, element 150).

It is respectfully submitted that the service server is independent of, and not connected to, the authentication server and the ticket granting server (see id., Fig. 2). Within the secure environment, the YAKSHA database of Ganesan is directly linked to the authentication server and the ticket granting server (see id.; col. 15, lns. 9-27). It is submitted that Ganesan does not disclose a direct link between the service server and either of the authentication server or the ticket granting server.

It is submitted that the system of Ganesan does not

disclose an authentication procedure wherein four messages (e.g., challenge 1, response 1, challenge 2, and response 2) are exchanged solely between two entities, as recited in independent claim 1.

Additionally, as understood by Applicants, Ganesan fails to disclose that response 1 sent from the terminal to the network is equal to challenge 2, whereby the network has requested response 2 together with challenge 1 and response 1 as a triplet data set, as recited in independent claim 1.

It is respectfully submitted that Schneier discloses only that keys may be random-bit strings generated by some automatic process (see Schneier, p. 173, lns. 19-23), and does not disclose the authentication procedure of the present application as described above.

It is therefore respectfully submitted that neither Ganesan nor Schneier, alone or in combination, disclose or suggest a method for mutual authentication of components in a network using a challenge-response method to authenticate a terminal with the network, comprising the steps of requesting at least one data pair including a first random number (Challenge 1) and a first response (Response 1) from an authentication center using a request from the network, passing the first random number (Challenge 1) to the terminal which calculates the first response (Response 1) based upon an internally stored key and the first random number (Challenge 1), sending the calculated first response (Response 1) to the network, and responding to a second random number with a second response (Response 2) calculated in the authentication

center, the response performed by the network, wherein the first response (Response 1) sent from the terminal to the network is also used as the second random number (Challenge 2), whereby the network has previously requested the second response (Response 2) from the authentication center together with the first random number (Challenge 1) and the first response (Response 1) as a triplet data set (Challenge 1/Response 1/Response 2), as recited in independent claim 1.

Accordingly, for at least the above-stated reasons, it is respectfully submitted that independent claim 1 is patentable over the cited references.

Withdrawal of the rejection of claim 1 under 35 U.S.C. § 103(a) is respectfully requested.

Reconsideration is respectfully requested of the rejection of claims 2-14 under 35 U.S.C. § 103(a), as allegedly being unpatentable over Ganesan and Schneier, and further in view of U.S. Patent No. 5,544,245 to Tsubakiyama.

In the remarks set forth on page 4 et seq., the Office Action apparently also refers to J. Clark et al., ''A Survey of Authentication Protocol Literature: Version 1.0,'' (1997) (hereinafter ''Clark et al.'').

Applicants have carefully considered the comments of the Office Action and the cited references, and respectfully submit that claims 2-14 are patentably distinct over the cited references for at least the following reasons.

It is submitted that independent claim 1, and the claims depending therefrom, including claims 2-14, are patentable over Ganesan in view of Schneier for at least the reasons set

forth above.

Tsubakiyama, as understood by Applicants, relates to a mutual authentication/cipher key delivery system in which a communication network and all of its users have devices for implementing a common key cryptosystem. Identifier ID_i of user i is made public in the network. An authentication key K_i of user i is known only to the network and the user, and each user generates a random number r_n for authentication of the network and sends it and his identifier ID_i to the network.

The network of Tsubakiyama inputs into a specific function F() the random number r_n received from the user and a random number r_u generated by the network itself, encrypts the resulting output value $F(r_n,r_u)$ by an encryption algorithm $E1K_i()$ using the authentication key K_i of the individual user as a cipher key and sends the encrypted data C_1 to the user.

The user of Tsubakiyama obtains D_1 by inputting the data C_1 into inverse function $E1K^{-1}\ K_i()$ of the encryption algorithm $E1K_i()$ using the user's authentication key K_i as a cipher key, inputs D_1 into an inverse function $F^{-1}()$ of the function F(), and judges the network to be valid only when d_1 is equal to the random number r_n. It is respectfully submitted that the operation described above is completely different from the method of the present application.

Additionally, the Office Action states that in the method of Tsubakiyama the message C_1 sent from the network equates to a challenge, and that the response from the user i who interprets the alleged challenge responds with response C_2 (see Office Action, p. 4, lns. 6-9).

It is respectfully submitted that there is no indication in Tsubakiyama that the network interprets the message C_1 as the message C_2.

As understood by Applicants, Tsubakiyama discloses that the network N encrypts r_n // r_u, obtainable by the function F() of an authentication information processing function generator, by an encryptor in the ECB mode of the DES encryption algorithm, using as a cipher key the authentication key K_i of the user available from a database of K_i, the encrypted data C_1 of a 64-bit length being sent to the user (see Tsubakiyama, col. 4, lns. 43-51).

The user decrypts data C_1 by a decrypter in the ECB mode of the DES encryption algorithm, using authentication key K_i as a cipher key, obtains data D_1 by an authentication information processing inverse function generator, and makes a check by a comparator 8 to see if d_1 matches with r_n. When they do not match, the user judges the network to be a false network and stops the authentication protocol. When they match, the user judges the network to be an authorized network, newly generates the random number r_c by a random number generator, concatenates data d_2 and the random number r_c by a cryptographic key generating function generator to obtain d_2 // r_c as a cipher key k_c for cipher communication after authentication, encrypts d_2 // r_c by an authentication information processing function generator and an encrypter in the ECB mode of the DES encryption algorithm using the user's authentication key K_i as a cipher key and sends the encrypted data C_2 to the network (see id., col. 4, ln. 52 to col. 5, ln.

4).

It is respectfully submitted that the above-described method of Tsubakiyama does not disclose or suggest that the network interprets the message C_1 as the message C_2, as stated in the Office Action.

Regarding Clark et al., it is respectfully submitted that the method of Clark et al. does not disclose or suggest the use of two challenge values and two response values for authentication, as recited in independent claim 1.

In contrast, in the mutual authentication method of the present invention, as recited in amended independent claim 1, at least one data pair including a first random number (Challenge 1) and a first response (Response 1) are requested from an authentication center using a request from the network. The first random number (Challenge 1) is passed to the terminal which calculates the first response (Response 1) based upon an internally stored key and the first random number (Challenge 1), and the calculated first response (Response 1) is sent to the network. The network responds to a second random number with a second response (Response 2) calculated in the authentication center, wherein the first response (Response 1) sent from the terminal to the network is also used as the second random number (Challenge 2), and whereby the network has previously requested the second response (Response 2) from the authentication center together with the first random number (Challenge 1) and the first response (Response 1) as a triplet data set (Challenge 1/Response 1/Response 2).

Furthermore, it is respectfully submitted that the method of Clark et al. does not disclose or suggest that the first response corresponds to the first random number.

In contrast, in the present invention, the first random number (Challenge 1) is passed to the terminal, and the terminal calculates the first response (Response 1) based upon an internally stored key and the first random number (Challenge 1), as recited in independent claim 1.

Additionally, in the method of the present application, the first response (Response 1), calculated in the terminal and sent from the terminal to the network, is used as the second random number (Challenge 2). The network is not required to send another random number to the terminal. The required random number (Challenge 2) is available in the terminal, as it corresponds to the first response (Response 1) which has been calculated by the terminal (see specification of the present application, p. 4, lns. 11-19).

In the method of the present application, the terminal does not produce the second random number (Challenge 2), but equates it to the second response (Response 2) (see id., p. 4, ln. 20 to p. 4a, ln. 5). The network therefore produces a second response and sends it to the terminal, which compares it to the value in the terminal to determine if the network is authentic (see id.).

Accordingly, for at least the above-stated reasons, it is respectfully submitted that independent claim 1, and the claims depending therefrom, including claims 2-14, are patentable over the cited references.

Withdrawal of the rejection of claims 2-14 under 35 U.S.C. § 103(a) is respectfully requested.

Should the Examiner disagree, it is respectfully requested that the Examiner specify where in the cited document there is a basis for such disagreement.

The Office is hereby authorized to charge any fees which may be required in connection with this amendment and to credit any overpayment to Deposit Account No. 03-3125.

Favorable reconsideration is earnestly solicited.

Respectfully Submitted,

Dated: January 21, 2005

I hereby certify that this paper is being deposited this date with the U.S. Postal Service as first class mail addressed to:
Commissioner for Patents
P.O. Box 1451
Alexandria, VA 22313-1450

1/21/05
Norman H. Zivin Date
Reg. No. 25,385

Norman H. Zivin
Registration No. 25,385
c/o Cooper & Dunham LLP
1185 Avenue of the Americas
New York, New York 10036
(212) 278-0400
Attorney for Applicants